20 | WAF：如何为漏洞百出的Web应用保驾护航?

2020-01-29 何为舟

讲述：何为舟
时长 12:59 大小 11.89M

你好，我是何为舟。

如果你细心观察的话，应该会发现，随着 Web 应用越来越多，黑客的攻击目标也逐渐转向了针对 Web 安全的攻击。传统的防火墙主要专注于网络层的攻击防御，对 Web 安全的防御能力相对欠缺。因此，WAF（Web Application Firewall，Web 应用防护系统）的概念也就被提了出来。WAF 说白了就是应用网关防火墙的一种，它只专注于 Web 安全的防御，近几年来逐渐被当成一个相对独立的产品方向来研究。

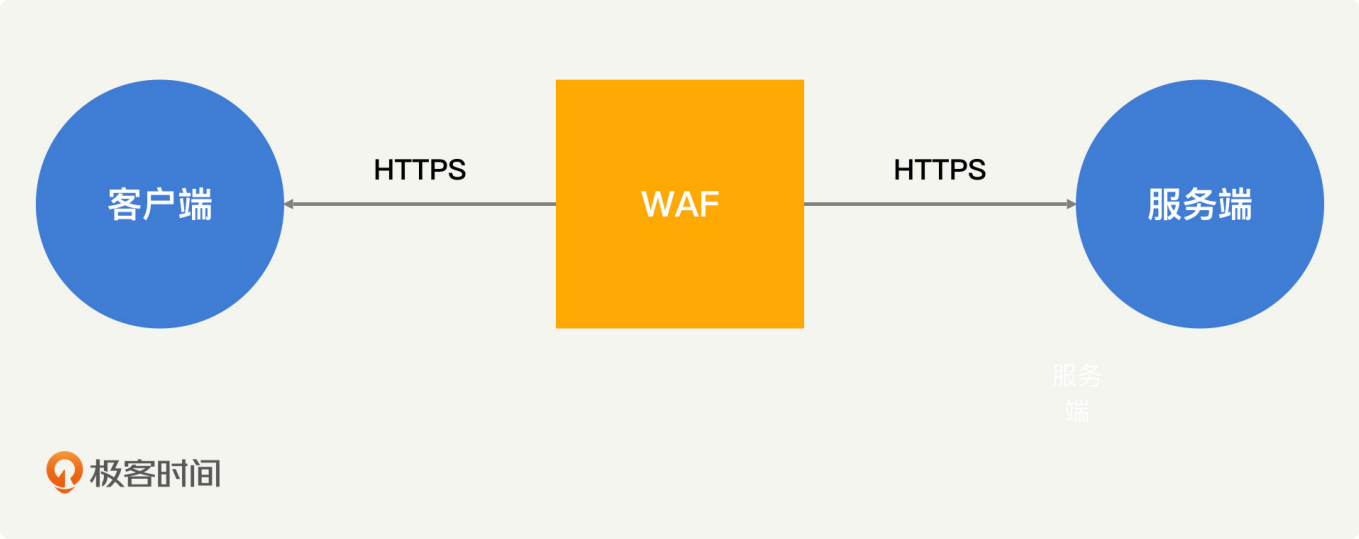
那么，WAF 和防火墙到底有哪些区别呢？针对我们之前讲过的各种 Web 攻击手段，WAF 是如何提供保护的呢？今天，我们就一起来看！

WAF 的工作模式

前面我说过，WAF 的本质是“专注于 Web 安全的防火墙”，Web 安全关注于应用层的 HTTP 请求。因此，WAF 的分析和策略都工作于应用层。

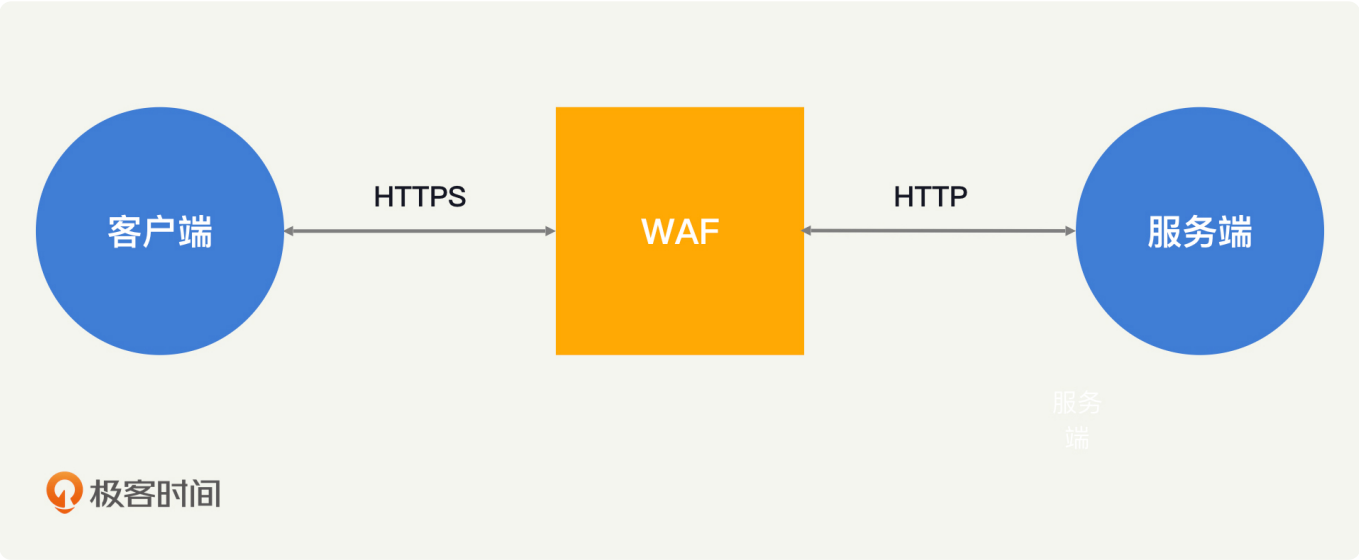
在 Web 安全这个方向上，WAF 对比防火墙又做出了哪些改进呢？我们可以从 WAF 的三种工作模式入手，探讨这两者的区别。这三种工作模式分别是：透明代理、反向代理和插件模式。

透明代理和大部分防火墙的工作模式相同：在客户端和服务端通信不需要作出任何改变的情况下，对 HTTP 流量进行请求和转发。在这个过程中，为了解密 HTTPS 流量，WAF 必须和服务端同步 HTTPS 对称密钥。



透明代理的优点就是容易部署，它不需要客户端和服务端进行任何改动。但是，透明代理的缺点也有很多。透明代理本身不是一个 Web 服务，所以它无法修改或者响应 HTTP 的请求，只能够控制请求的通过或者拒绝。正因为如此，它也无法实现 Web 服务所提供的认证、内容过滤等功能。

区别于透明代理，反向代理要求客户端将请求的目标地址指向 WAF，而不是服务端。在反向代理工作模式中，服务端接收的请求，实际上也是由 WAF 发起的。在这个过程中，WAF 本身就相当于一个 Web 服务，只不过对所有的 HTTP 请求都进行了转发。



因为**反向代理 WAF 本质上是一个 Web 服务**，所以 HTTPS 证书可以直接部署在 WAF 上。WAF 在对 HTTPS 流量解密之后，就可以在内网中用 HTTP 的形式，向服务端发起代理请求了。

而且，反向代理 WAF 作为一个 Web 服务，能够提供的功能也更加丰富。比如，WAF 可以充当一个前置的认证平台，对所有请求进行身份校验和身份管理。同时，也因为在反向代理工作模式中，客户端和服务端不直接通信，而是将全部请求都先请求到 WAF 上，所以反向代理 WAF 对服务端的隔离也更加彻底。

但是，反向代理同样存在缺点。首先，功能更丰富意味着性能开销更大。因此，反向代理 WAF 对硬件要求更高。其次，反向代理 WAF 一旦宕机，就无法响应客户端的任何请求。这样一来，即使服务端仍然正常，但用户已经无法正常使用应用了。而对于透明代理 WAF 来说，如果 WAF 宕机了，只是无法提供 Web 防护而已，客户端和服务端的通信不会受到任何影响。

最后，我们来看**插件模式**。在插件模式中，WAF 不再是网络中一个独立的安全产品了，而是以插件的形式依附于 Web 服务端本身，为 Web 安全提供防护。

那怎么才能将 WAF 植入到服务端的逻辑中呢？我们最常使用的一种技术就是 AOP（Aspect Oriented Programming，面向切面编程）技术。在 AOP 技术中，WAF 可以作为一个切片植入到服务端的逻辑中。

而且，目前 AOP 技术十分流行，各类编程语言都支持。所以，插件模式的 WAF 部署同样十分简单。但是，这种将 WAF 和服务端强耦合的方式，会带来一定的负向影响。

首先，WAF 和服务端一块工作在服务器上，会消耗服务器额外的资源，对 Web 服务本身的性能产生影响。

其次，WAF 和服务端耦合，也就意味着 WAF 的所有改动都会直接影响到服务端。对于代理模式的 WAF 来说，通常只需要自测就可以升级了。而对于插件模式的 WAF，它本身的升级必须和服务端一起进入评估和测试流程，就会增加额外的工作量。

为了帮助你理解这三种工作模式，我总结了一张表格。

模式	特点	优势	劣势
透明代理	1.和传统防火墙类似 2.需要和服务端同步HTTPS密钥	1.部署简单，无需任何改动	1.处理方式只有通过或者拦截，不能进行修改
反向代理	1.本质上是一个Web服务 2.可以直接部署HTTPS证书	1.功能丰富 2.隔离彻底	1.性能相对较低 2.高可用受到影响
插件模式	1.本质上是一个切片 2.和服务端强耦合	1.部署简单，服务端通过AOP技术引入即可 2.高可用由服务端提供	1.对服务端性能产生影响 2.升级流程更加严格

极客时间

总结一下，关于 WAF 的三种工作模式，你需要重点掌握这些内容：首先，WAF 将处理的请求协议限定为 HTTP，所以 WAF 比应用网关防火墙具备更高的专业性和灵活性；其次，WAF 可以以代理的形式，在网络中提供 Web 安全防护，也可以作为插件嵌入到服务端中；最后，我们也可以根据需求、成本和硬件环境等因素，选择不同的部署模式对 Web 安全进行防护。

WAF 的功能

在了解 WAF 的主要工作模式之后，我们知道，在部署模式上 WAF 比防火墙具备更高的灵活性。WAF 可以根据不同的需求，以不同的形式为 Web 服务提供保护。同样的，在功能上，WAF 也可以去实现一些 HTTP 请求中特有的安全功能。比如去解析 HTTP 数据、解密 HTTPS 流量等。下面，我们就来看一下，WAF 到底有哪些功能服务？

1. HTTP 解析能力

我们知道，WAF 专注于 Web 安全。因此，对 HTTP 请求进行解析是 WAF 最基础的能力。在 HTTP 中，通用的内容包括：请求的 URL 以及其中的参数、HTTP 头部信息、POST 的 body 内容等。

除此之外，某些攻击特征可能隐藏得比较深，比如 JSON 中的某个字段，无法通过 JSON 的整体内容检测出来，我们必须一个字段一个字段去判断。因此，WAF 还需要解析 XML、JSON 等 RPC 传输协议，能够理解对应的 key 和 value 分别是什么。

除了单纯地解析内容，WAF 还需要对 HTTP 内容做必要地处理。为什么要这么做呢？这主要有两方面原因。

第一，HTTP 中的内容可能经过了 UrlEncode 等编码方式的处理，因此，**WAF 需要具备解码能力，避免攻击的特征通过编码来进行绕过**。

第二，**想要看到 HTTPS 中的加密内容，WAF 必须能够解密 HTTPS 请求**。在透明代理模式中，WAF 需要和服务端同步 HTTPS 的密钥，才能够获得解密的请求；在反向代理中模式中，WAF 自带证书，可以直接解密；在插件模式中，WAF 依靠服务端解密请求之后，再进行 HTTP 的解析。

2. Web 安全防护

通过对 HTTP 请求进行解析、对编码内容进行解码和对 HTTPS 进行解密之后，WAF 就能够获得全部 HTTP 请求内容了。在此基础之上，WAF 就可以对请求内容进行分析，为 Web 服务提供安全保护了。

我总结了三种主要的分析手段。

签名匹配：和杀毒软件中病毒库的概念类似，WAF 也可以维护一个攻击样本库。样本库中存有已知攻击请求的散列签名，只要 HTTP 请求内容的散列签名在这个样本库，就说明 HTTP 请求中携带了攻击内容。

正则匹配：签名匹配需要请求完全一致才能够检测出来，而正则匹配只需要部分特征就可以检测。WAF 可以通过抽象一些攻击特征的正则表达式，对 HTTP 请求进行检测。比如，如果请求的某个参数中出现了单引号，那么很有可能就是黑客发起的 SQL 注入攻击。

行为分析：除了针对单次请求的分析之外，WAF 还可以针对连续的访问请求特征进行提取和分析。为什么要这么做呢？这是因为，很多时候，我们无法准确判断单次请求是不是攻击请求，但是如果疑似的攻击请求频繁出现，我们就基本能够确定了。也就是说，一个用户不会频繁地访问同一个页面，而黑客需要对一个漏洞点发起多次尝试，才能够实现攻击的效果。

在识别到攻击的请求之后，WAF 就可以对请求进行拦截，从而避免 Web 服务受到黑客的攻击了。

3. 审计告警

WAF 还有另外一个重要的功能，就是为 Web 服务提供安全相关的审计和告警功能。Web 安全相关的审计包括：发生攻击的时间、路径、频次等。通过这些信息，开发人员能够知道自己的 Web 服务面对的攻击威胁是什么样的，也就能够更好地评估威胁，完善 Web 安全防护机制。

除此之外，WAF 还能提供其他的审计能力。这是因为，WAF 能够解析出 HTTP 请求的全部内容，提供审计所需要的全部日志字段。这些日志可以是各个页面的访问次数、用户的访问行为和接口的响应性能等。尽管这些指标和安全没有太多关系，但是它们对于产品设计和服务质量来说都很常见，那么 WAF 就可以作为一个统计分析工具，来为你提供服务。

4. 数据保护和虚拟补丁

反向代理或者插件模式的 WAF，还能够对 HTTP 请求中的数据进行一定的处理，提供额外的数据保护功能。

最简单的，WAF 可以加密 HTTP 响应中的 Cookie 内容，使得 Cookie 以保密的形式存储在浏览器中。当浏览器将加密后的 Cookie 附加到 HTTP 请求中的时候，WAF 又可以进行解密。这样一来，服务端接收到的始终是明文的信息，而实际上，WAF 通过加解密为 Cookie 提供了额外的保护。另外，WAF 还可以对返回内容中的手机号、身份证号等敏感字段进行统一的打码处理，避免因为开发的疏忽，导致这些敏感信息的泄漏。

在介绍插件漏洞的时候，我们提到了防火墙可以提供虚拟补丁的功能，来临时对插件漏洞进行修复。如果插件是 Web 相关的服务，那么 WAF 是不是也可以提供虚拟补丁的功能呢？当然是可以的。那 WAF 是如何提供虚拟补丁的呢？我来举个简单的例子。

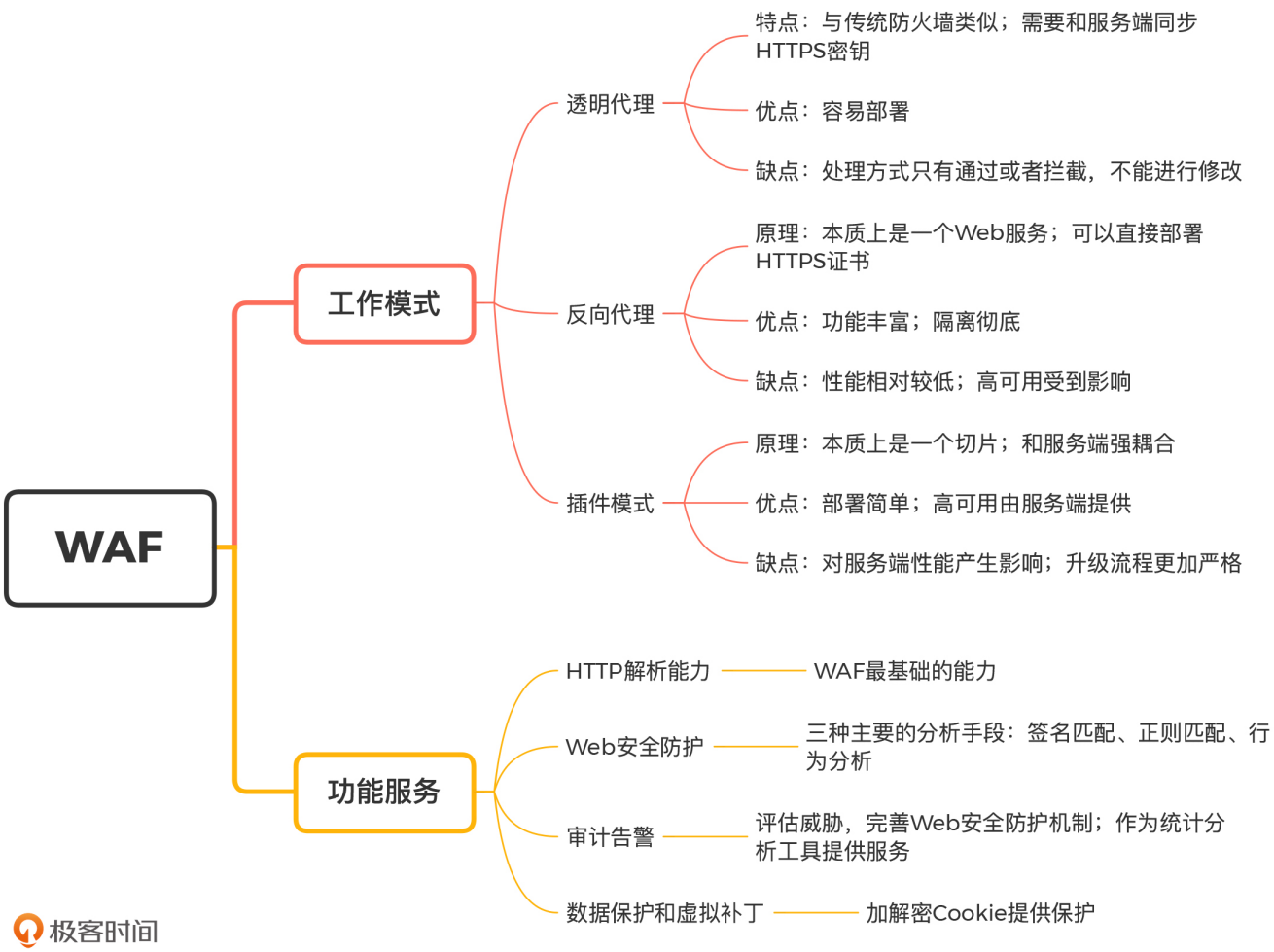
在经典的 Structs 2 漏洞中，黑客是通过 Structs 2 中包含的漏洞接口发起攻击的。所以，WAF 只需要将这些包含漏洞的接口进行封禁，或者对请求内容中的 Structs 2 攻击特征（特定接口的异常序列化数据）进行分析拦截，就能够临时避免 Structs 2 受到已公开的漏洞攻击。之后，我们只需要对 Structs 2 进行升级再打上补丁，这样就可以下线虚拟补丁了。

总结

好了，今天的内容讲完了。我们来一起总结回顾一下，你需要掌握的重点内容。

在今天的课程中，我们主要介绍了 WAF 的工作模式和主要功能。简单来说，WAF 就是专注于 Web 安全的防火墙，它能够以透明代理、反向代理和插件的模式，运行在网络和系统的各个环节中。从功能上来说，WAF 能够解决绝大部分的 Web 安全问题，对于黑客针对 Web 的攻击进行分析和拦截，同时提供额外的审计告警、数据保护等能力。

同样地，在选取 WAF 的时候，我们首先需要考虑功能的完整性和易用性。公司能够以较低的成本部署 WAF，并解决大部分的 Web 安全问题，这是 WAF 最关键的效果。其次，就是可配置和可维护性，对于漏过的攻击请求如何进行补充完善，对于误判的请求如何进行放行，这是我们在使用 WAF 过程中必然会遇到的问题。一个好的 WAF 产品应该提供友好的入口，供开发和运维人员对漏过和误判的规则进行维护。



思考题

最后，给你留一道思考题。

任何安全产品都不可能达到 100% 的安全。你可以思考一下，在 Web 安全中，黑客能够通过哪些方式绕过 WAF 的检测和过滤呢？

欢迎留言和我分享你的思考和疑惑，也欢迎你把文章分享给你的朋友。我们下一讲再见！

© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇　19 | 防火墙：如何和黑客“划清界限”？

下一篇　模块串讲（一） | Web安全：如何评估用户数据和资产数据面临的威胁？

精选留言 (6)

写留言

宝仔
2020-02-01

现代基于k8s微服务的架构下,用哪种模式的WAF会更好呢？微服务下一般会有一层网关，网关可能是基于java的spring gateway，也可能是基于openresty(nginx+Lua)的Kong，想问下这种模式下怎么设计WAF更加友好点？望老师能做回复

展开

宝仔
2020-01-31

现在的WAF一般都是nginx+lua来实现的把?

展开

tt
2020-01-29

绕过WAF也是用双拼和闭合么?

展开

小晏子
2020-01-29

可以从安全防护的地方入手，如WAF通过正则匹配进行行为检测，那么可以考虑能不能绕过正则匹配或者让其匹配失效，比如通过提交非常大的数据，使其数据量超过WAF的能够正则匹配字符，那就可以不经过WAF的正则匹配了。

展开

大侠
2020-01-29

市面上都有哪些主要WAF产品等，各有什么优缺点，就更好了。

leslie
2020-01-29

这个东西其实早就被广泛使用了：具体原理用途都大致知道，记忆中这东西应当有和nginx一起使用，真实的作用还是第一次如此学习；受教了。

展开